Electronic Signatures

Defining the gamut of technology available for Electronic Signatures

presented by:

Office of the Secretary of State

Michael Totherow, Chief Information Officer

Russ Savage, Electronic Transactions Liaison

Secure Transactions

- security of the electronic signature at time of transaction
  - i.e., securing the creation of the evidence
- security of the electronic document over the life of the transaction
  - i.e., securing the evidence over time

Secure Electronic Signature

- UETA

44-7031. Secure electronic signatures

A signature is a secure electronic signature if, through the application of a security procedure, it can be demonstrated that the electronic signature at the time the signature was made was all of the following:

1. Unique to the person using it.
2. Capable of verification.
3. Under the sole control of the person using it.
4. Linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.

Secure Electronic Record

- UETA

44-7032. Secure electronic records

If, through the ongoing application of a security procedure, it can be demonstrated that an electronic record signed by a secure electronic signature has remained unaltered since a specified time, the record is a secure electronic record from that time of signing forward.

- Not only at time of reception, but over life of evidence!

Security and Risk

- Security is a response to risk
  - Categories of Risk Assessment:
    - Monetary
    - Reputation
    - Productivity
- Government's role is to maintain the reputation of individuals in society
  - unfortunately the hardest risk to assess

Risks associated with the Creation of the Evidence

1. Authentication - know who it is

2. Access control - manage what they can do once you know who it is

3. Confidentiality - keep secret what shouldn't be shared (including in transit)

4. Integrity - no damage to data

5. Non-repudiation - hold-up-in-court proof of they said yea or nay on the transaction

Risks associated with the life of the Evidence

1. Theft of valuable information

2. Direct financial loss from fraud

3. Loss of business opportunity

4. Unauthorized use of resources

5. Loss of customer confidence or respect (citizens, other government entities, etc.)

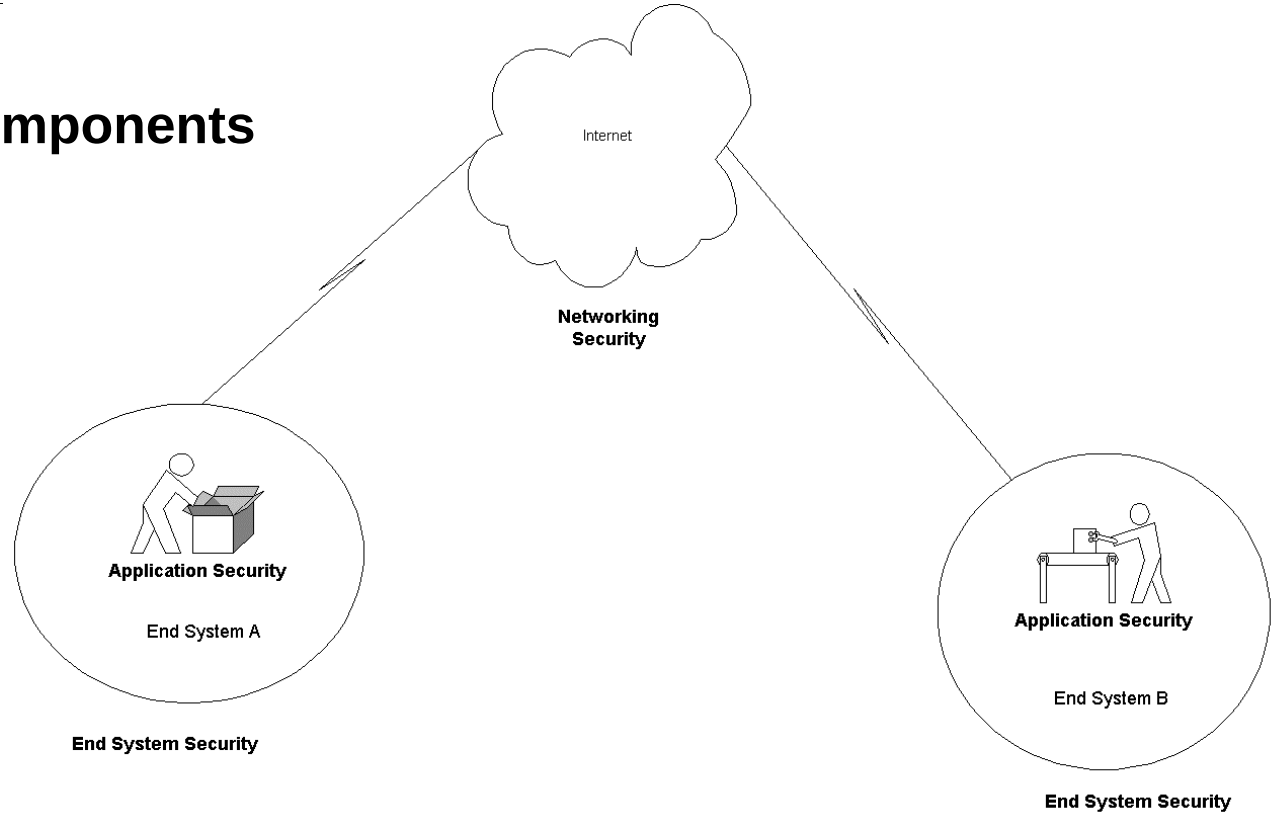
6. Cost caused by uncertainties (interruptions,by whatever cause, lead to uncertainty and stalled transactions)

7. False information provided (misinformation)

Security and Transactions

- Individual risks gives us guiding principles of protection
- Categories of risk give us importance of security
- Process is meeting the criteria with acceptable risk
  - unique to the person
  - capable of verification
  - under sole control
  - linked to the record in such a manner if the record is changed, the signature is invalid
- For most processes, these will occur in electronic transactions on the Internet

Internet Security Components



1. ***Network security*** (the Internet “plumbing” between points A and B - where A & B are “end systems”)
2. ***End System security*** (the non-Internet “plumbing” -the PC or computer network at point A or point B)
3. ***Application security*** (the application may have security separate from the network and the end systems)

[Note that all the security services could be required by any of the three Internet security components.]

[A Virtual Private Network (VPN) is a process of establishing sufficiently secure services at both end-systems and on the network so that points A & B can act like a single end-system]

Type of “applications” that might require security

1. Messaging (e.g. e-mail: SMIME, MOSS, etc.)
2. Sensitive Information -
   Financial/Commerce & formal Government Information Exchanges

   (e.g. auto manufacturer's EDI network)

   (e.g. the credit card SET infrastructure)

   (e.g. state/local law enforcement interaction with the FBI & other national agencies)
3. Web site - secure interaction (e.g. SSL & S-http)

   (SSL uses "hidden" PKI for encryption & authentication)

   (may be secure enough [or hide some security services] to do financial/commerce apps without the more formal EDI or SET infrastructure)
4. Electronic documents - acknowledgment signing, committing by electronic signature

   (e.g. PKI/XML based procurement process)

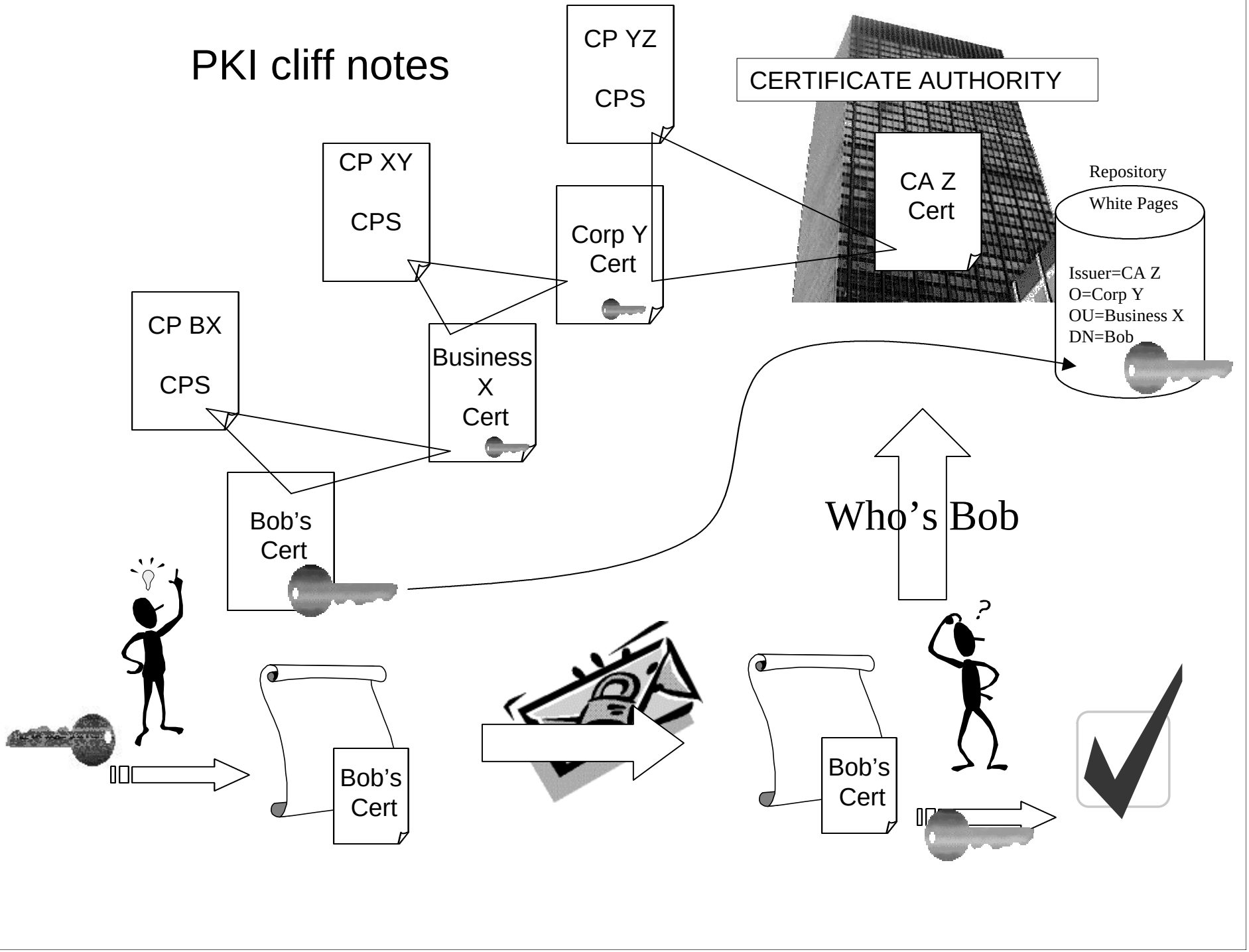
Looking at technology to meet the ES needs

- We know the categories of risk and some potentials
- We know the general security points to address them
  - client (environment, application, identity)
  - transmission (interception, alteration, positive negative)
  - reception (authentication, imposter, denial)
  - processing (environment, application, storage, access)
  - retention (environment, storage, access)
- We know the criteria of evidence
- How do the different signing processes match up?

Public Key Infrastructure

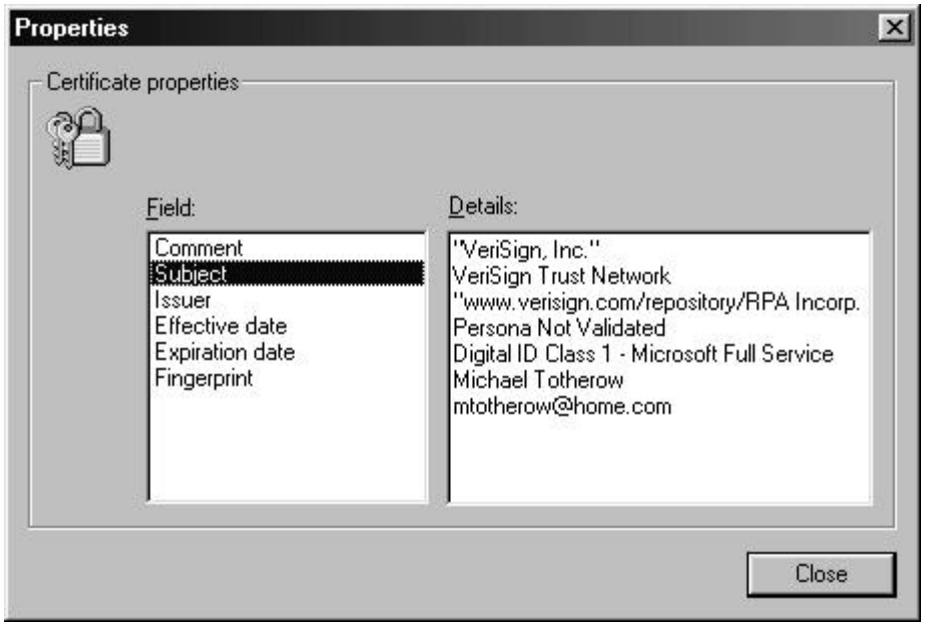
- Description of a trust through Certificate Policies & Certificate Practice Statements
  - hierarchy of organizational units and end nodes
  - uses x.509v3 certificates as protocol specification
  - responsibilities and liabilities of the members of the network
  - governs the operational aspect (tech and process) of Infrastructure
- uses a public / private key combination to allow
  - Identity
  - Hierarchy
  - Encryption

PKI cliff notes



Digital Signatures (PKI)

- uses a certificate issued within a PKI
  - here's what a certificate looks like
  - elements of a certificate
- uses encryption algorithms
  - publicly known algorithms
  - very high levels of assurance
- Bits equates stronger protection, but encryption still decays with age



Digital Signature in Four corner model

- Subscriber
  - Enters network by association or by need to interact with network
  - Requires in-person challenge to enter network
  - Agrees to abide by rules of trust network
- Certification Authority
  - Certification Registrar
    - Challenges the subscriber's identity
    - Can be third party or 'owners' of network - the agencies
  - Certification Issuer
    - Traditional Certification Authority generates keys
    - Maintains security of keys
    - Vendor chosen off of Approved Certification Authority List

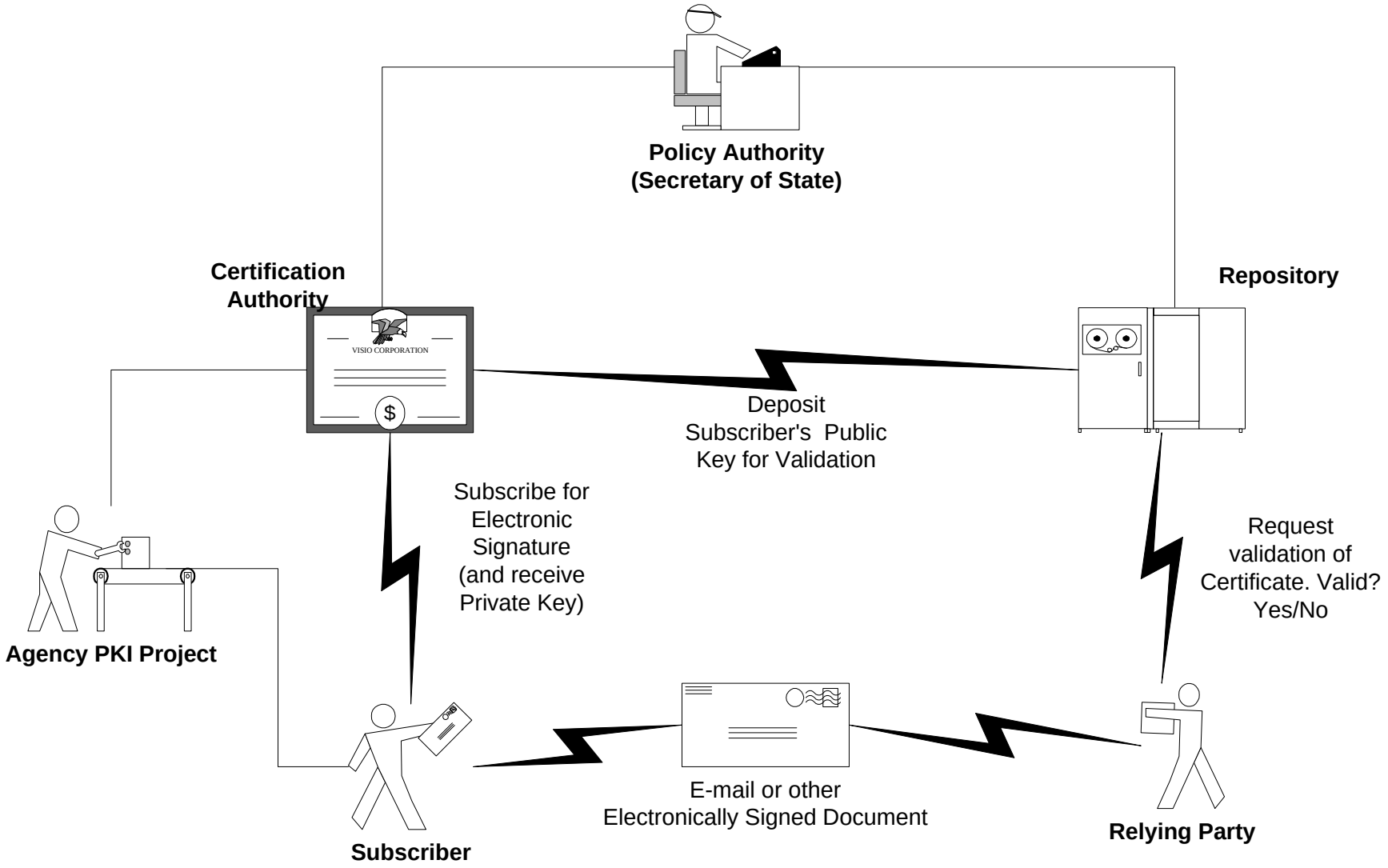
Digital Signature in Four corner model

- Repository
  - Publicly accessible, inside and outside of network
    - May be maintained by Certification Authority or
    - May be maintained by central authority - the state
  - Secured by PKI
- Relying party
  - ‘Government’ is reliance
  - Defines the PKI (trust network) through CP selection
  - Enters into contractual arrangement with CA
    - for repository needs?
    - Archival needs?
    - Registration duties?
    - Other services?

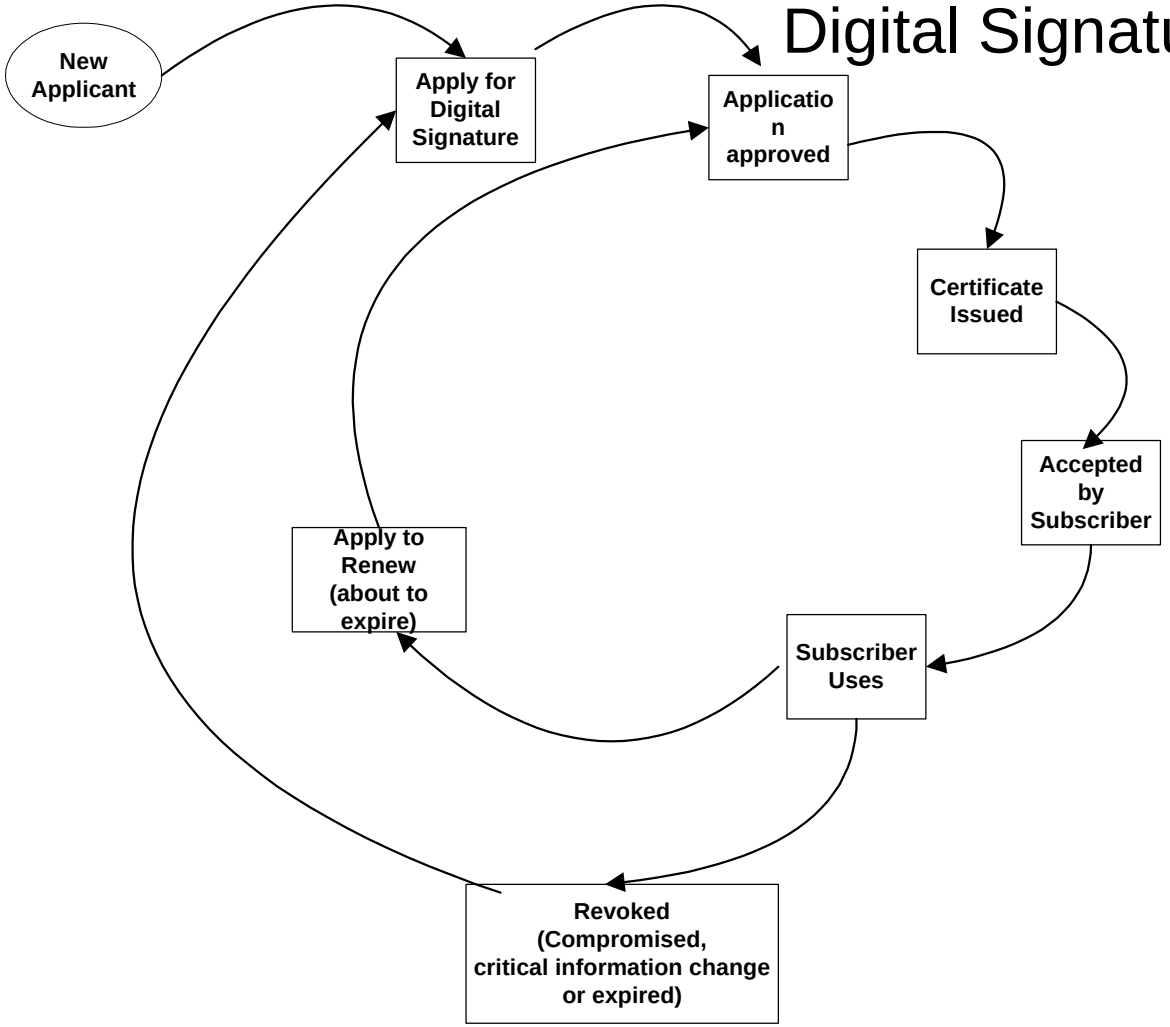
PKI signature example

1. Policy Authority defines the Certificate Policy for trusted network description
2. Government as a relying agency defines community of interest
    a. Chooses technology - Digital Signature
    b. Chooses Certificate Policy
    c. Chooses Vendor off Approved Certification Authority List
        i Gov will act as RA
        ii Gov will archive certificates
        iii Vendor sells tool sets to subscribers
    d. Gov creates application for community
3. Subscriber visits Registration Authority (potentially Gov through contract) to register
    a. Subscriber verifies identity to RA
    b. CA issues digital signature to Subscriber
    c. Subscriber gets training from Vendor
    d. Subscriber installs tool set with Vendor support
4. CA publishes public digital signature in Repository
5. Subscriber uses application to commit transaction
    a. Signs document with issued digital signature
6. Relying party (Gov) receives document
    a. Verify integrity of transaction
        i Verify signature against repository
        ii Check Certificate Revocation List (CRL)
    b. Updates database and stores transaction
        I Information parsed and saved in db
        ii “document” stored for evidence
    c. Receipt sent to subscriber
    d. Relying party verifies receipt received

The Roles in Electronic Signature Use
(State of Arizona's infrastructure model)



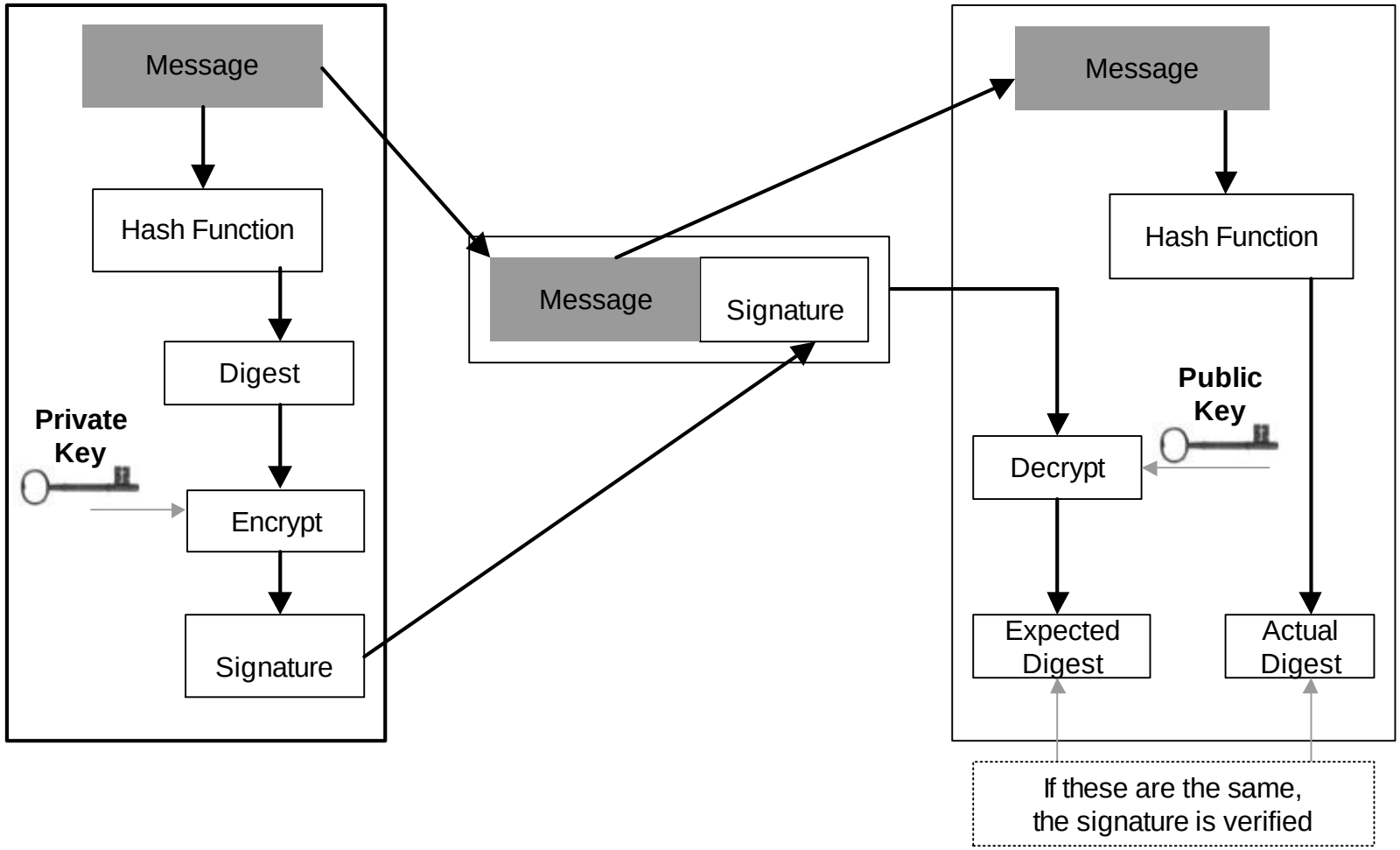
Digital Signature Life Cycle



Digital Certificate Life Cycle

While this describes PKI certificates, the need for application and renewal occurs for any electronic signature process - you have to identify the applicant and periodically renew them

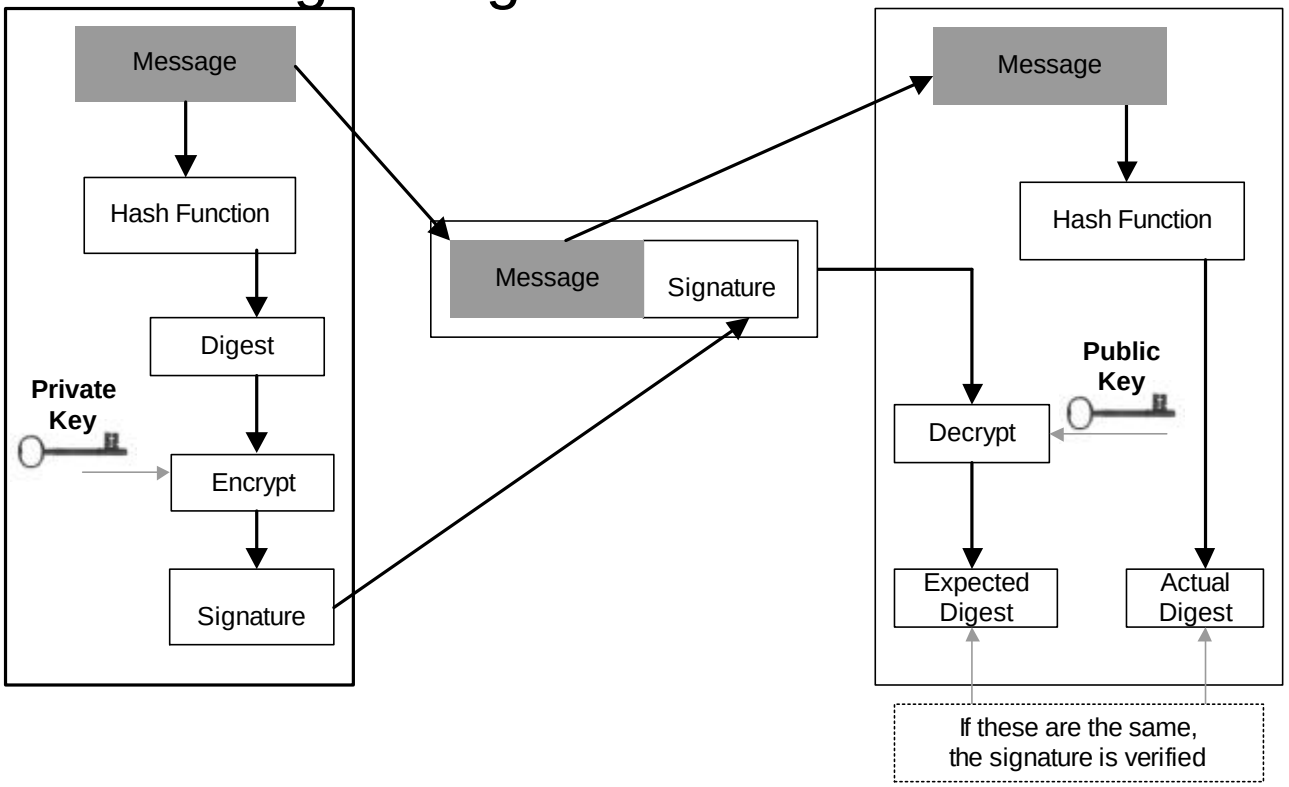
Digital Signature “how”



Sam can send a message to Jean. Jean will know it is from Sam and that the message has not been altered.

This is “Hi, I sent this and you know whether it was changed.

Digital Signature “validation”



An electronic signature

shall be unique to the person using it,

shall be capable of reliable verification and

shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

Arizona Statute 41-132 B

PKI Risk evaluation

- Uniqueness
  - In-person registration assures uniqueness
- Verifiable
  - provides non-refutable verification
    - Repudiation based on handling, not technology
- Sole control
  - Combination something person knows with have = Medium
  - Smart card could be next to perfect (with biometric)
    - depends on implementation
- Linked to the record
  - Implementation inherent by design

Electronic Document by DS

SAMPLE SIGNING BLOCK

```
[s01] <Signature Id="MyFirstSignature"
      xmlns="http://www.w3.org/2000/09/xmldsig#">
[s02]  <SignedInfo>
[s03]  <CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
[s04]  <SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
[s05]  <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
[s06]   <Transforms>
[s07]     <Transform
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
[s08]   </Transforms>
[s09]   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[s10]   <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
[s11]  </Reference>   [s12] </SignedInfo>
[s13]  <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
[s14]  <KeyInfo>
[s15a]   <KeyValue>
[s15b]    <DSAKeyValue>
[s15c]      <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
[s15d]    </DSAKeyValue>
[s15e]   </KeyValue>
[s16]  </KeyInfo>
[s17] </Signature>
```

```
<xml version=1.0>

<document>

   <title>An Electronic Document</title>

   <Section style=paragraph>This is an example of a document.</Section>

   <Section style=paragrahp>Everything within the document tag is passed to the hash algorithm to create the hash.  The hash is stored in the document under the signing block, and the digital signature certificate information is inserted to designate who “signed” the document.</Section>

</document>

<Signature Id=“Mike Totherow” xmlns=“http://repository.verisign.com/clm#1”>

 <SignedInfo>

<CanonicalizationMethod
       Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
 <SignatureMethod
       Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
 <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
       </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
 </Reference>   [s12] </SignedInfo>
 <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
 <KeyInfo>
   <KeyValue>
     <DSAKeyValue>
       <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
     </DSAKeyValue>
   </KeyValue>
 </KeyInfo>
</Signature>
</xml>
```

Email Digital Signature

Received: from femail18.sdc1.sfba.home.com ([24.0.95.145]) by extra.sosaz.com with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21)
id JFJH9NQG; Sat, 28 Apr 2001 13:39:06 -0700
Received: from cx74747a ([24.1.194.228]) by femail18.sdc1.sfba.home.com
(InterMail vM.4.01.03.20 201-229-121-120-20010223) with SMTP
id <20010428204109.YZEE937.femail18.sdc1.sfba.home.com@cx74747a>
for <mtotherow@sos.state.az.us>; Sat, 28 Apr 2001 13:41:09 -0700
Message-ID: <006101c0d023$2e530780$03019dc0@phnx3.az.home.com>
From: "Michael Totherow" <mtotherow@home.com>
To: "Michael Totherow" <mtotherow@sos.state.az.us>
Subject: This is a Signed Email
Date: Sat, 28 Apr 2001 13:38:20 -0700
MIME-Version: 1.0
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=SHA1;
boundary="----=_NextPart_000_005C_01C0CFE8.7DBBDD00"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200

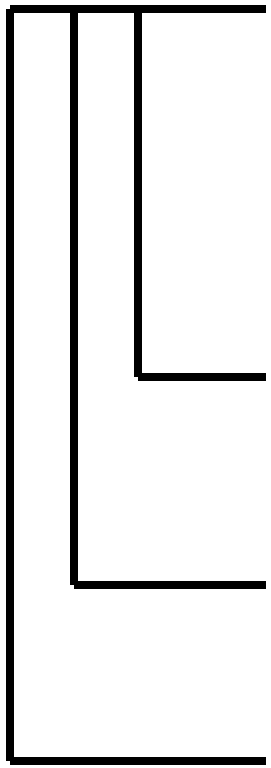
This is a multi-part message in MIME format.

------=_NextPart_000_005C_01C0CFE8.7DBBDD00
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

------=_NextPart_000_005C_01C0CFE8.7DBBDD00
Content-Type: application/x-pkcs7-signature;
name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="smime.p7s"

------=_NextPart_000_005C_01C0CFE8.7DBBDD00--

Enveloping



<DOCUMENT>
<PARAGRAPH>
BLAH BLAH BLAH
</PARAGRAPH>
</DOCUMENT>
<SIGNATURE>
<SIGNATURE_BLOCK ID=1>
SIGN HERE
</SIGNATURE_BLOCK ID=1>
<SIGNATURE_BLOCK ID=2>
SIGN HERE
</SIGNATURE_BLOCK ID=2>
<SIGNATURE_BLOCK ID=3>
SIGN HERE
</SIGNATURE_BLOCK ID=3>
</SIGNATURE>

Pretty Good Privacy

- uses a certificate - basically for encryption
  - certificate looks like digital certificate, but no authority
  - certificate is self generated
- uses encryption algorithms
  - publicly known algorithms, and some proprietary
  - levels of assurance based on application
- Bits equates stronger protection, but process is more subject to security breach

PGP in Four corner model

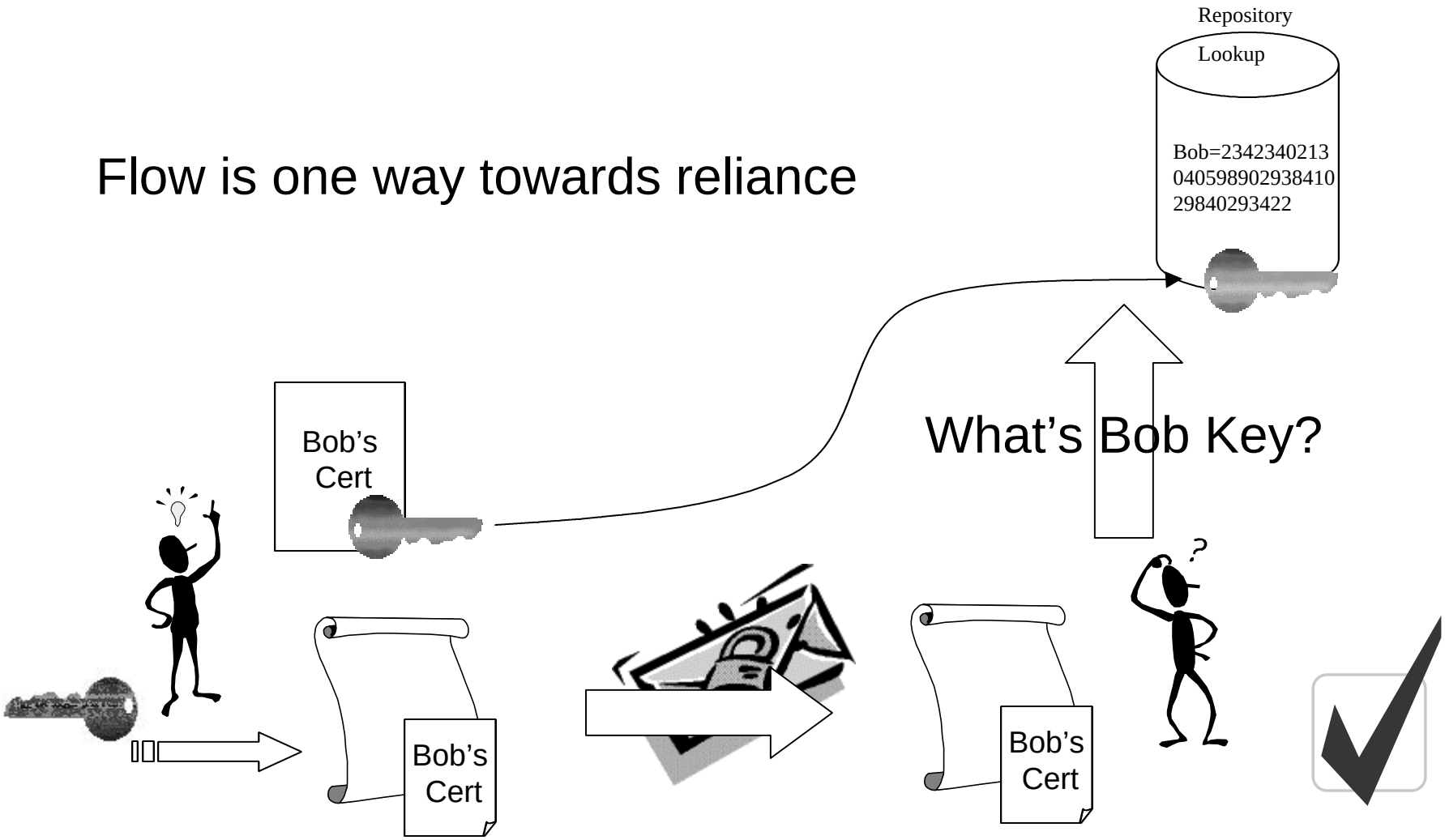
- Subscriber
  - agrees to participate using technology and process of application
  - Self describes and self identifies to community
- Certification Authority
  - Certification Registrar
    - does not exist. Willing to participate is the registration, so only suited to well known communities with inherent trust
  - Certification Issuer
    - self administered. Typically the specification for technology details which certificates and with what elements need to be present

PGP in Four corner model

- Repository
  - Publicly accessible
    - not publicly accessible
    - PGP depends of static relying party
      - so repository only readable from relying party
      - write only from subscribing party
  - Secured private network
- Relying party
  - Government is reliance
    - sets standard and security level for community
    - possibly distributes tool set / application

PGP Signature example

Flow is one way towards reliance



PGP Signature example

1. Policy Authority defines the Certificate Policy for trusted network description
2. Government as a relying agency defines community of interest
    a. Chooses technology - PGP Signature
    b. Chooses Certificate Policy
    c. Chooses Vendor/Tool Set for implementing PGP
        i Gov will act as RA by only accepting transactions from whom they care to
        ii Gov will archive PGP certificates
        iii Government specifies tool sets for subscribers
    d. Gov defines specification of application for community
3. Subscriber visits Gov to indicate they will participate
    a. Subscriber gets tool set
    b. Subscriber either acquires application or meets specification
    c. Subscriber responsible for meeting specification
    d. Subscriber signs contract with Relying party for participation in community
4. Subscriber uses application to commit transaction
    a. Generates digital signature
    b. Submits digital signature to Repository to store (Gov or third party)
    c. Signs document with application with digital signature
    d. Submits digital signature according to specification
5. Relying party (Gov) receives document
    a. Verify integrity of transaction
        i Filing meets specification
        ii Verify signature against repository
        iii Verifies identity against internal list of community
    b. Updates database and stores transaction
        i Information parsed and saved in db
        ii digital signature downloaded and stored
        iii “document/record” stored for evidence
        iv “document/record” linked to signed contract between parties
    c. Receipt sent to subscriber
    d. Relying party verifies receipt received

PGP Risk Evaluation

- Uniqueness
  - Self registration questions uniqueness
    - process dependent
  - since we talking about electronic signatures
    - highest regard of electronic identity
    - results in very contextual application
- Verifiable
  - provides next to non-refutable verification
    - Repudiation based security of uniqueness process
- Sole control
  - Combination process and uniqueness
- Linked to the record
  - Implementation dependent
- Not recommended for non-repudiation transactions -- especially subject to rebut

Shared Secret Signing

- may or may not use a certificate
  - if uses certificate is only for interfacing with encryption routines
- uses encryption algorithms
  - mostly privately known algorithms, distributed to community
    - could use publicly known, but then “shared secret” becomes a very weak link
  - levels of assurance dependent upon community and risk of breach of community
- Bits typically do not equate stronger protection, but privacy of transactions are more subject to security breach

Shared Secret in Four corner model

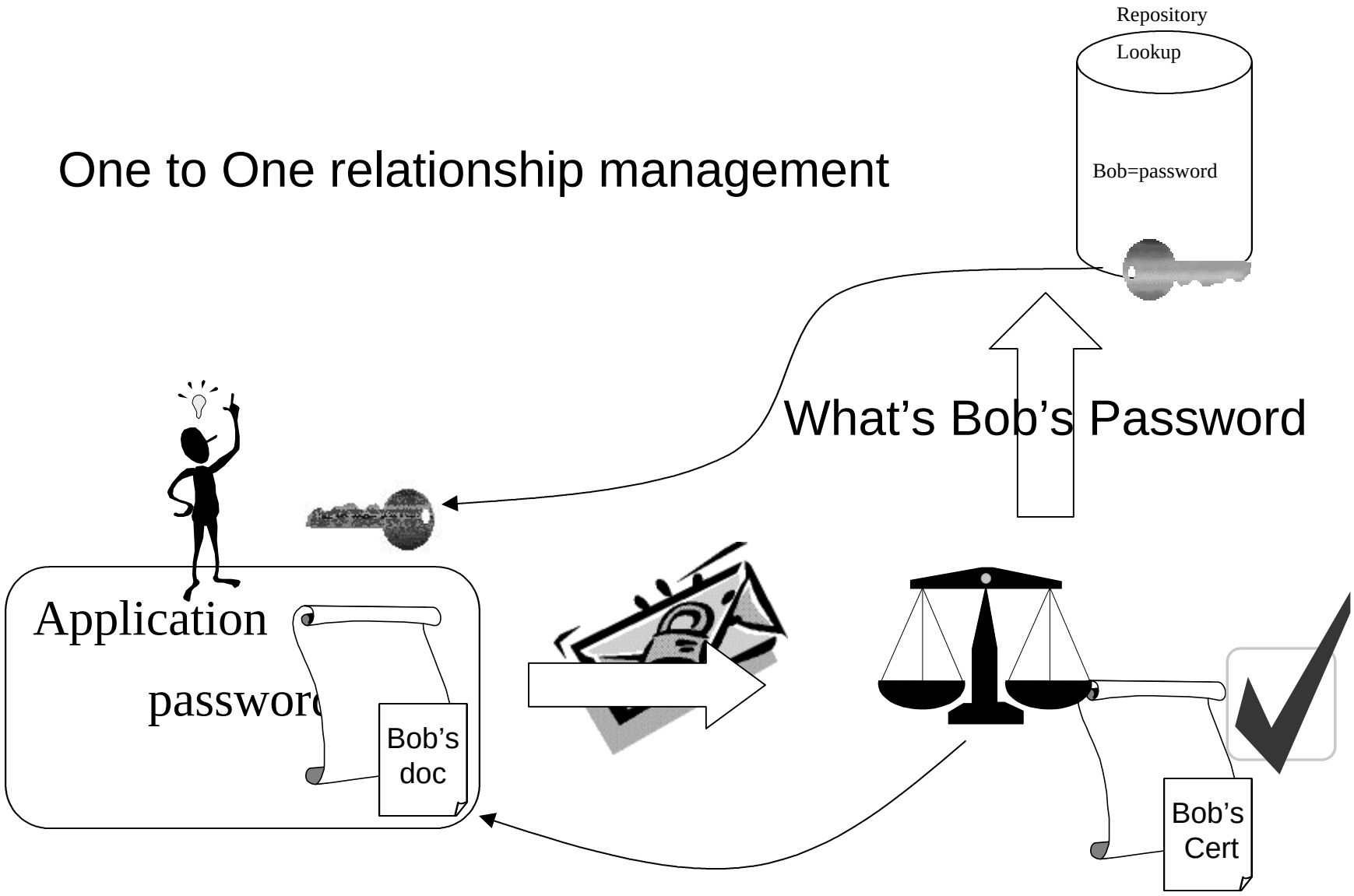
- Subscriber
  - Explicit community revolving relying party
  - agrees to participate using tool set (or application) specified, often provided by relying party
  - Identified solely by relying party, secret creates one to one relationship
- Certification Authority
  - Certification Registrar
    - Relying party registers subscriber by “contract” into community
  - Certification Issuer
    - Shared Secret issued by relying party to subscribing party
      - variation of shared secret submitted by relying party breaks contract dependence of who is authority

Shared Secret in Four corner model

- Repository
  - Publicly accessible
    - not publicly accessible
    - Shared secret depends on security of relying party repository of shared secrets
      - so repository only readable and write-able from relying party
  - Secured private network
- Relying party
  - Government is reliance
    - sets standard, typically designs shared secrets and levels of security
    - distributes tool set or application

Shared Secret Signature example

One to One relationship management



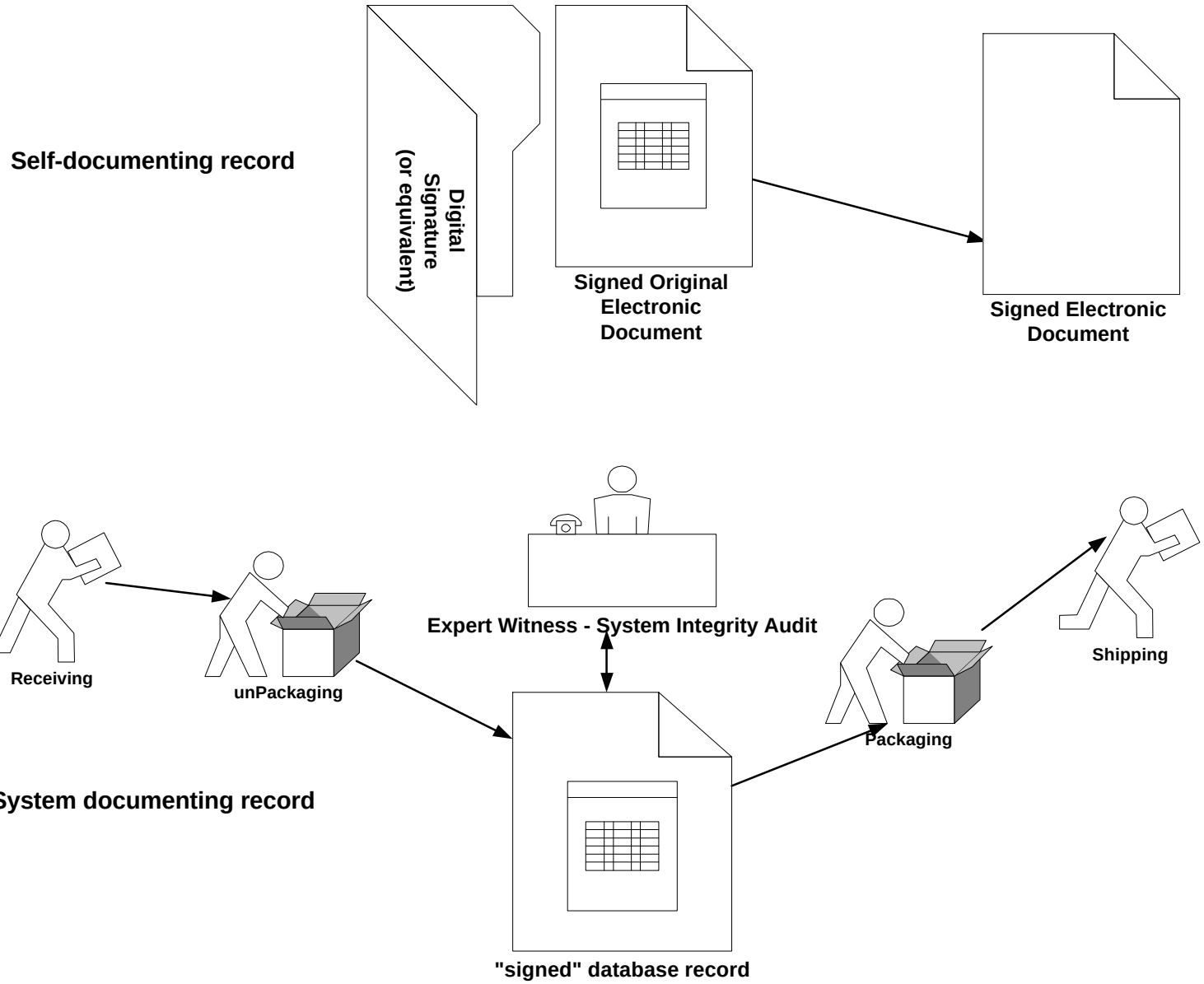
Shared Secret Signature example

1. Policy Authority defines the Certificate Policy for trusted network description
2. Government as a relying agency defines community of interest
    a. Chooses technology - Shard Secret Signature
    b. Chooses Certificate Policy
    c. Creates “contract” to be basis of evidence for signing to be signed by subscriber i
    Gov will act as RA by contracting with subscriber directly
        ii Gov will ensure security of community and shared secrets
    d. Gov creates application and secured network connections for operation
3. Subscriber visits Gov to indicate they will participate
    a. Subscriber signs contract
    b. Subscriber either acquires application or meets specification
    c. Subscriber responsible for meeting specification
    d. Subscriber held to maintaining security in community
4. Subscriber uses application to commit transaction
    a. Signs document with application with digital signature
5. Relying party (Gov) receives document
    a. Verify integrity of transaction
        i Filing meets specification
        ii Verify signature against repository of shared secrets
        iii Verifies identity against internal list of community
    b. Updates database and stores transaction
        i Information parsed and saved in db
        ii digital signature downloaded and stored
        iii “document/record” stored for evidence
        iv “document/record” linked to signed contract between parties
    c. Receipt sent to subscriber
    d. Relying party verifies receipt received

Shared Secret Risk Evaluation

- Uniqueness
  - Relying Party sole registration assures uniqueness of identity
    - process dependent
- Verifiable
  - Process dependent
    - Repudiation based on sole control
- Sole control
  - Heavily questioned - password
- Linked to the record
  - Implementation dependent
- Weakest link is scale and maintenance
  - managing shard secrets horrendous
  - cost of management rises with participation
- Liability falls upon Relying party
  - security of community is sole responsibility
- Applicable to small communities where reliance is internal only, not external

The goal… Evidence



Evidence in these Technologies

- self documenting keeps the evidence useable
- trustworthy systems are dependent on the entire environment

- Must consider all elements which may detract from integrity of evidence

Evidence in PKI

Essential elements:

- Evidence of the origin of the message
- Evidence of sent
- Evidence of receipt
- Timestamp as needed of origin, sent, receipt
- Long-term storage of evidence
- Designated adjudicator of prospective disputes

- The signed document
  - open standard XML applicable to document definition
    - contains origin, date created (formalized/sent)
  - application of server's digital signature builds history into document
    - contains origin, date received (formal reception/acknowledgement time stamp)
    - timely updates of date stamped integrity
- Document's life cycle independent of environment
  - migrate-able avoid technical rendering resolve
  - transferable to another authority

Evidence in PGP

Essential elements:

- Evidence of the origin of the message
- Evidence of sent
- Evidence of receipt
- Timestamp as needed of origin, sent, receipt
- Long-term storage of evidence
- Designated adjudicator of prospective disputes

- The signed document
  - proprietary standard (perhaps XML) definition
    - contains origin (requires alternate verification link), date created (formalized/sent)
  - application at server stores history in journal
    - contains origin (with link) , date received (formal reception/acknowledgement time stamp)
    - timely updates of date stamped integrity of integrity of system
    - audit log of access to journal system
    - audit of control of signing repository for linking “sole control”
  - application that creates the document
    - Rendering control
- Document’s life cycle dependent of environment
  - migration may depend on technical change
  - transferable to another authority requires transferring control of entire record set

Evidence in Shared Secret

Essential elements:

- Evidence of the origin of the message
- Evidence of sent
- Evidence of receipt
- Timestamp as needed of origin, sent, receipt
- Long-term storage of evidence
- Designated adjudicator of prospective disputes

- The signed document
  - proprietary standard definition
    - contains origin, date created (formalized/sent)
  - application at server into system journal
    - contains origin, date received (formal reception/acknowledgement time stamp)
    - integrity based on original encryption (must store original encryption and “key”)
  - server journal
  - shared secret repository journal
  - system security audit
- Document’s life cycle dependent of environment
  - not migrate-able, possibly not verifiable if technology changes
  - transferable to another authority requires transfer complete record set

Context makes or breaks your process

- Regardless of technology, the process is the key to electronic signatures
- Re-think the process
  - First question to ask: Why a signature?
    - Requirement comes from?
  - Second question to ask: Why the signature?
    - Intent to process?